

REMARKS/ARGUMENTS

Upon entry of the present amendment, claims 1, 2, 4-19 remain pending in this application, of which claims 1, 11, 12, 14, 16, and 17 are amended. Applicants respectfully submit that that no new matter has been added by the present amendment. Claims 1, 2, 7, and 9 stand rejected under 35 U.S.C. § 103(a) as allegedly being anticipated by U.S. Patent No. 6,167,517 ("Gilchrist") in view of U.S. Patent No. 6,202,151 ("Musgrave"). Claims 4-6, 8, 10-13, 17, and 20 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Gilchrist in view of Musgrave as applied to claims 1, 2, 7, and 9 above, in view of U.S. Patent No. 6,310,966 ("Dulude") and further in view of U.S. Patent No. 5,280,527 ("Gullman"). Claims 14-16, 18, and 19 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Gilchrist in view of Musgrave in view of Dulude and further in view of Gullman as applied to claims 4-6, 8, 10-13, 17, and 20 above and further in view of U.S. Patent No. 6,092,201 ("Turnbull"). Applicant respectfully requests reconsideration of the present application in light of the below recited remarks.

Rejections Under 35 U.S.C. § 103

Claims 1, 2, 7, and 9

Claims 1, 2, 7, and 9 stand rejected under 35 U.S.C. § 103(a) as allegedly being anticipated by Gilchrist in view of Musgrave. Applicant respectfully disagrees.

Newly amended independent claim 1 includes a feature neither taught nor suggested by

the prior art, namely “an encryptor coupled to the security code generator to encrypt the signed biometric data.”

The present invention is directed to systems and methods for securely transmitting and authenticating biometric data over a network. In an embodiment of the invention, a biometric sample is collected at a sensor and sent from the sensor to an authentication server so that a biometric template may be generated from the biometric sample at the authentication server. To ensure the authenticity of the imaging device, the biometric sample is signed with a signature of the sensor prior to being transmitted to the server. Also, to ensure that the signed biometric sample is not corrupted in transit to the server, the signed biometric data is also encrypted with a server public key. Thus, the present invention provides a dual protection and authentication system, with a biometric sample that is **both** signed with a sensor signature and encrypted with a server public key.

By contrast, Gilchrist discloses systems and methods for trusted biometric authentication. Gilchrist discloses that:

“[a] host system receives an identifier for the user from a client system. This identifier is used to retrieve a template containing biometric data associated with a user, and this template is returned to the client. The client then gathers a biometric sample from the user, and compares this biometric sample with the template to produce a comparison result. Next, the client computes a message digest using the template, the comparison result and an encryption key, and sends the message digest to the host system. This computation takes places within a secure hardware module within the client computing system that contains a secure encryption key in order to guard against malicious users on the client system. Next, the host system receives the message digest and authenticates the user by determining whether the message digest was computed using the template, the encryption key, and a comparison result indicating a

successful match between the biometric sample and the template (Gilchrist, Col. 2, lines 27-45).”

Thus, Gilchrist discloses sending a data package including a biometric comparison result from a client to a host.

As noted by the Examiner in the Official Action, Musgrave discloses creating a digital signature by encrypting a hashed value with a private key (Col. 2, ln. 23-25). However, Musgrave does not disclose encrypting signed data.

Importantly, the cited references do not teach a biometric sample that is both signed with a camera signature and encrypted, as recited by newly amended claim 1. Applicant respectfully requests that the Examiner cite where in the cited references there is any mention of both signing and encrypting a biometric sample.

Applicant respectfully submits that dependent claims 2, 7, and 9 are patentable at least by reason of their dependency.

Claims 4-6, 8, 10-13, 17, and 20

Claims 4-6, 8, 10-13, 17, and 20 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Gilchrist in view of Musgrave as applied to claims 1, 2, 7, and 9 above, in view of Dulude and further in view of Gullman. Applicant respectfully disagrees.

Newly amended independent claim 11 includes a feature neither taught nor suggested by the prior art, namely: “an encryptor to encrypt signed data using the public key.”

Newly amended independent claim 17 includes features neither taught nor suggested by the prior art, namely: “encrypting the signed data package using the server public key certificate.”

Gilchrist discloses sending a data package including a biometric comparison result from a client to a host (Gilchrist, Summary of the Invention).

Dulude discloses encrypting transaction data and a user’s sample biometric data with the user’s private key and transmitting the encrypted data from a sending device to a receiving device. At the receiving device, the encrypted data may be decrypted and the user’s identity may be authenticated using the user’s pre-stored biometric data (Dulude, Summary of the Invention).

Gullman discloses the use of a biometric token for authorizing access to a host system. The token includes a comparison between a biometric input from a user and a template (Gullman, Summary of the Invention).

Importantly, the cited references do not teach a biometric sample that is both signed with a camera signature and encrypted, as recited by newly amended claims 11 and 17. Applicant respectfully requests that the Examiner cite where in the cited references there is any mention of both signing and encrypting a biometric sample.

Applicant respectfully submits that dependent claims 4-6, 8, 10, 12, and 13 are patentable at least by reason of their dependency.

Claims 14-16, 18, and 19

Claims 14-16, 18, and 19 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Gilchrist in view of Dulude and further in view of Gullman and further in view of Turnbull. Applicant respectfully disagrees.

Newly amended independent claim 14 includes a feature neither taught nor suggested by the prior art, namely: “encrypting the signed biometric data.”

Turnbull discloses that a receiving party may authenticate a public key of a sending party by using the sending party’s signature public key certificate obtained from a certification authority (Turnbull, Col. 1, line 64 - Col. 2, line 2).

Importantly, the cited references do not teach a biometric sample that is both signed with a camera signature and encrypted, as recited by newly amended claim 14. Applicant respectfully requests that the Examiner cite where in the cited references there is any mention of both signing and encrypting a biometric sample.

Applicant respectfully submits that dependent claims 15, 16, 18, and 19 are patentable at least by reason of their dependency. Accordingly, reconsideration and withdrawal of the 35 U.S.C. § 103(a) rejections are respectfully requested.

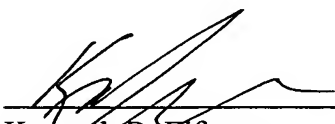
DOCKET NO.: IRID-0479
Application No.: 10/020,791
Office Action Dated: December 31, 2003

PATENT

CONCLUSION

In view of the above remarks, Applicant respectfully submits that the present application is in condition for allowance. Reconsideration of the application and an early Notice of Allowance are respectfully requested.

Date: May 28, 2004



Kenneth R. Eiferman
Registration No. 51,647

Woodcock Washburn LLP
One Liberty Place - 46th Floor
Philadelphia PA 19103
Telephone: (215) 568-3100
Facsimile: (215) 568-3439